IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA)
)
Plaintiff,) Civil Action No.
)
v.) **FILED *EX PARTE***
) **AND UNDER SEAL**
EVGENIY MIKHAILOVICH BOGACHEV,)
et al.)
Defendants.)

DECLARATION OF SPECIAL AGENT ELLIOTT PETERSON IN SUPPORT OF APPLICATION FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

I, Elliott Peterson, declare as follows:

1. I am a Special Agent with the Federal Bureau of Investigation in Pittsburgh, Pennsylvania. I make this declaration in support of the United States of America's Application For An Emergency Temporary Restraining Order And Order To Show Cause Re Preliminary Injunction. I make this declaration of my own personal knowledge or on information and belief where noted and, if called as a witness, I could and would testify completely to the truth of the matters set forth herein.

2. I currently investigate criminal and national security computer intrusions in the Pittsburgh Field Office Cyber Squad. I have been a member of the Cyber Squad for two years. As such I have been trained in investigative tools and techniques required to pursue criminals employing sophisticated online tools such as botnets, Distributed Denial of Service attacks (DDOS), and Virtual Private Networks (VPN).

I. BACKGROUND

3. As used herein, the following terms have the following meanings :

a. "Malware" is malicious software, usually loaded onto a computer without the knowledge of the computer's owner or user. For example, computer viruses are malware.

b. A "botnet" is a network of computers that cyber criminals have infected with malware that gives a cyber criminal access to each computer and allows a cyber criminal to control each computer remotely.

c. A "botmaster" is a cyber criminal controlling a botnet.

d. A "credential harvester" is malware that finds and captures a victim's online credentials, which a cyber criminal can then use for purposes such as posing as the victim and initiating fraudulent financial transfers.

e. An Internet Protocol (IP) address is the unique address of a computer or other device connected to a network, and is used to route Internet communications to and from the computer or other device.

f. A "man-in-the-middle" attack is a cyber intrusion in which a cyber criminal causes a false website to be displayed to a victim attempting to access a legitimate website, such that the victim believes the false site to be the legitimate site. The false site asks for login credentials and/or personal information, which the cyber criminal captures without the victim's knowledge. The attack permits the victim to communicate back and forth with the legitimate website, but both captures the information flowing back and forth and can ask the victim for more information than the legitimate website would.

g. "Money mules" are individuals recruited by criminals for the express purpose of using the mules' accounts to launder stolen funds.

h. "Peer-to-peer" refers to a means of networking computers such that they communicate directly with each other, rather than through a centralized management point.

A. Overview of Gameover Zeus

4. My primary responsibility for the past two years has been the investigation of the Gameover Zeus (GOZ) botnet. GOZ, also known as "Peer to Peer Zeus," is one of the most

sophisticated computer viruses in operation today. Functioning primarily as a "credential harvester" and launching point for "man in the middle" attacks, GOZ is the latest incarnation of the Zeus malware, a credential stealer that first emerged in 2007, and has caused direct and indirect losses to consumers and businesses exceeding $100 million. GOZ contains a built-in suite of tools that allow botnet operators almost universal access to a victim's computer and any Internet content the victim can access from it. Security researchers estimate that between 500,000 and one million computers worldwide are infected with GOZ, and that roughly 250,000 of those infected computers are active "bots" in the GOZ network at any given time. The remaining bots are also infected with the malware, but are "inactive" because, for example, they are not currently powered on or connected to the Internet. Internet Protocol (IP) geolocation tools indicate that approximately 25% of the infected computers are located in the United States. Infection rates vacillate due to a number of factors, to include volume and timing of infection campaigns.

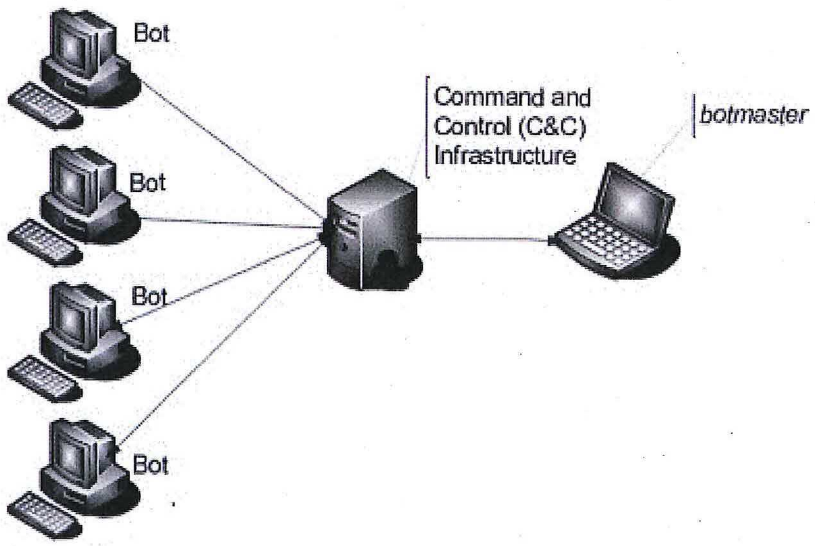
5. The principle purpose of GOZ is to capture banking credentials from infected computers, which the defendants then use those credentials to initiate fraudulent financial transfers from victims' bank accounts. The GOZ organization has also been known to change the recipients of otherwise legitimate payment orders. For example, on multiple occasions the operators of GOZ specifically targeted U.S. hospitals due to their large payroll payments. The operators would change the payroll beneficiaries from legitimate hospital employees, such as doctors and nurses, to "money mules." These co-opted transactions have been for substantial amounts; the stolen hospital payrolls were typically in the hundreds of thousands of dollars.

6. In terms of dollar amounts, the biggest threat represented by GOZ is the ability to utilize a victim's banking credentials to send nearly instantaneous wire payments to international beneficiaries. Based upon my interviews with security representatives from U.S. banks, industry experts in malware, and vendors of financial services platforms such as e-banking, I learned the prevalent tactics, techniques, and procedures employed by the GOZ operators, as well as the techniques utilized by the financial services industries to mitigate them. Most U.S. companies utilize their corporate financial accounts to send payments, either to employees or to vendors. Wire payments, according to the SWIFT wire payment system, is one such payment system employed by most U.S. banks. The GOZ operators discovered a mechanism by which to send international payments while avoiding all of the traditional safeguards associated with transmitting wires internationally. The amounts stolen in each wire transaction ranged from hundreds of thousands of dollars to 6.9 million dollars.

7. It is difficult to fully capture the extent of financial loss associated with GOZ, principally based upon the technical hurdles of directly attributing a given financial fraud directly with a specific malware strain. Most financial institutions struggle with differentiating these types of fraud, especially given the commonality of the many Zeus derived malware variants. However, based upon my training and experience, interviews with victims, technical monitoring of GOZ botnet activities, and examining the records kept by GOZ operators, it is my belief that total losses associated with GOZ exceed 100 million in the U.S. alone. The single largest known loss was a 6.9 million dollar wire. But fraudulent wires in the amount of 1 million dollars were very common. Examining the transactional logs for one U.S. bank able to specifically differentiate GOZ related fraud, reveals over 8 million dollars in loss over a 13

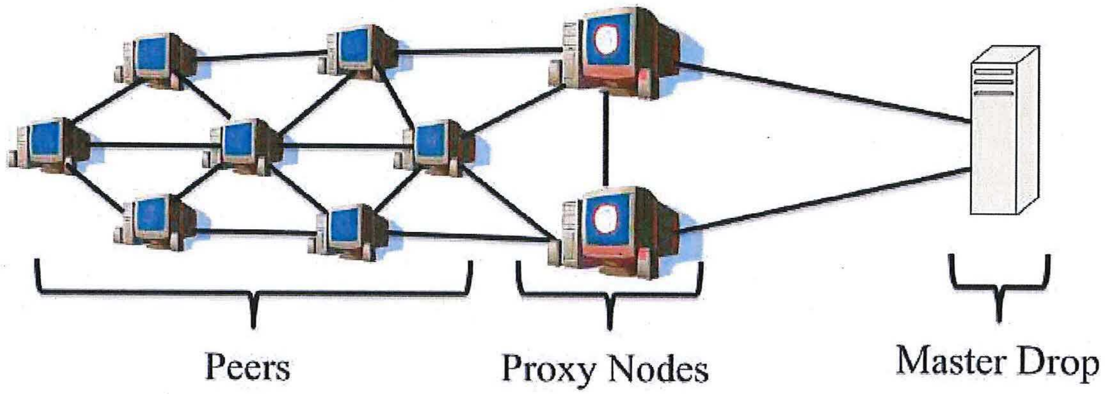
month period beginning 7/12/2012. Of a total of 11 fraudulent wires, six were for more than $950,000, with the largest wire being 2 million dollars. Exposure, a term used to describe to total residual value within financial accounts illegally accessed by GOZ operators, exceeded two billion dollars. These numbers are similar to the losses at other banks which retain equivalent records.

8. GOZ operates under a peer-to-peer framework that is designed to frustrate efforts to free infected computers from the GOZ botnet. Traditional botnets rely on a small number of centralized chokepoints known as Command and Control Servers that the "botmaster" can use to push commands to, and receive information from, infected bots. The diagram below illustrates how a traditional botnet functions:



9. From a criminal's perspective, a traditional command and control architecture is very simple to operate, but is also very vulnerable to disruption and seizure, since any interference between the command and control nodes and the victims will render the infected

bots free from the criminal's control. The GOZ architecture is a direct response to this vulnerability, spurning a centralized command and control system for one in which every infected computer is now a part of the command and control architecture, utilizing bot-to-bot communication to traffic stolen data. This architecture includes three layers. First, infected computers in the botnet are known as "peers," and maintain connections to each other. Second, a select number of peers, numbering in the thousands, are elevated to "Proxy Node" status. Proxy Nodes serve as relay points for commands coming from GOZ operators and for encrypted data stolen from the victim computers that is being directed to the GOZ operators. The GOZ operators can promote any GOZ-infected computer to Proxy Node status; Proxy Nodes generally appear to be selected based upon how long the computer has been part of the botnet, location, and how long and often the node is available to the botnet. Third, the encrypted data is ultimately funneled to "Master Drop" servers for later collection by the GOZ operators. This decentralization and obfuscation significantly complicate law enforcement and remediation efforts. Below is a simplified illustration of the GOZ botnet:



B. GOZ is Used to Wiretap Victims and to Facilitate the Theft of Funds

10. Once a computer is part of the GOZ botnet, the defendants have a variety of powerful options to steal sensitive information from the computer and to execute fraudulent transactions, as well as to install additional malware. The primary method used is known as a "man-in-the-middle" attack, which allows the GOZ operators to intercept communications between the victim's computer and a legitimate website, such as an online banking website. To increase the effectiveness of the man-in-the-middle attack, GOZ is capable of injecting additional code into the victim's web browser that changes the appearance of the website the victim is viewing. For example, if a GOZ-infected user were to visit a banking website that typically requests only a username and password, the defendants could seamlessly inject additional form fields into the website displayed in the user's web browser that request the user's Social Security number, credit card numbers, and other sensitive information. Because these additional fields appear to be part of the legitimate website users elected to visit, users are often defrauded into supplying the requested information, which is promptly intercepted by GOZ and transmitted to the defendants.

11. One example of GOZ's sophistication is its ability to defeat an advanced security mechanism commonly used by online banking systems, known as "two-factor authentication." The fundamental principle behind two-factor authentication is the combined use of something static, such as a password, and something variable, such as a randomly generated sequence of numbers. Typically, the variable factor is generated by the service provider, such as a bank or e-mail service, and is transmitted directly to the user through a text message, smartphone application, or specialized keyfob. Because the variable factor changes frequently, and is

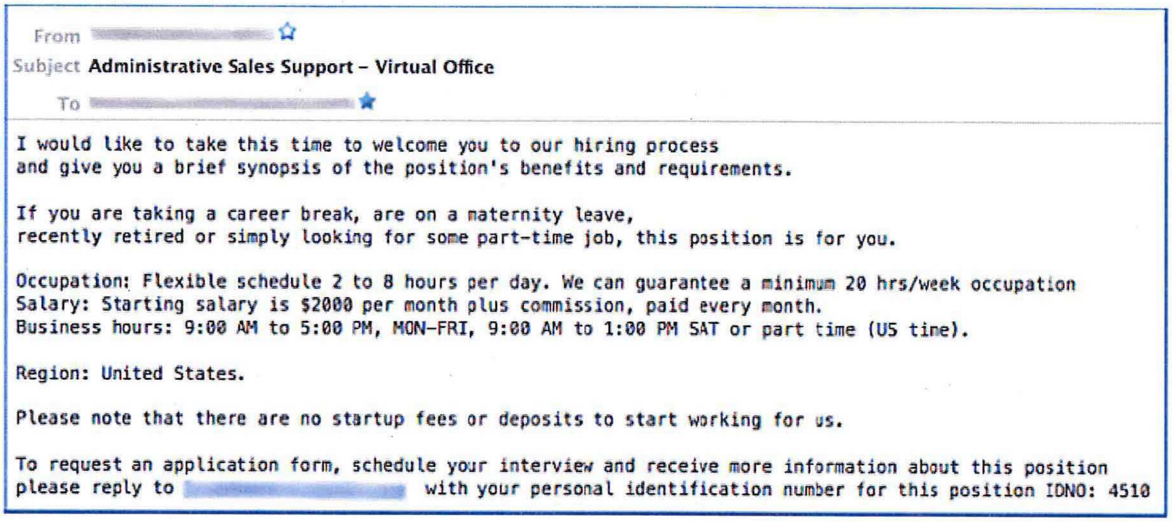
transmitted to a device in the user's physical possession, mere possession of a victim's user name and password—or capturing a victim's credentials at any one moment—are insufficient to fraudulently use those credentials.

12. GOZ, however, is sufficiently advanced that its operators can harvest both static and variable information in real time from the victims. Specifically, after the initiation of a man-in-the-middle attack, the GOZ operators will be queried by the bank for the variable portion of the victim's two factor initiation. The GOZ operators pass this query on to the victim in the form of a fictitious web injection. While the victim thinks that the information is being sent to the bank, it is instead sent directly to the GOZ operators.

13. After stealing victims' personal information, the defendants use the stolen credentials to log into victims' bank accounts and to initiate fraudulent electronic funds transfers from the victims' banks. This is most commonly done through the use of an Automated Clearing House ("ACH") payment or wire transfer sent to a money mule, from whom the funds are ultimately forwarded to the defendants.

14. Over the course of this investigation several money mules were interviewed. Money mules are usually recruited by the defendants through spam email campaigns, which promise lucrative jobs with flexible hours. In reality, the "job" offered to the prospective mules consists of nothing more than transferring stolen funds, which are wired to the mules' accounts after the defendants have raided victims' bank accounts. The defendants generally instruct the

money mules to keep a portion of the transferred funds as payment, and then wire the balance to a mule handler located overseas. A typical money mule recruitment email appears below:[1]



From [redacted]
Subject Administrative Sales Support – Virtual Office
To [redacted]

I would like to take this time to welcome you to our hiring process
and give you a brief synopsis of the position's benefits and requirements.

If you are taking a career break, are on a maternity leave,
recently retired or simply looking for some part-time job, this position is for you.

Occupation: Flexible schedule 2 to 8 hours per day. We can guarantee a minimum 20 hrs/week occupation
Salary: Starting salary is $2000 per month plus commission, paid every month.
Business hours: 9:00 AM to 5:00 PM, MON-FRI, 9:00 AM to 1:00 PM SAT or part time (US time).

Region: United States.

Please note that there are no startup fees or deposits to start working for us.

To request an application form, schedule your interview and receive more information about this position
please reply to [redacted] with your personal identification number for this position IDNO: 4510

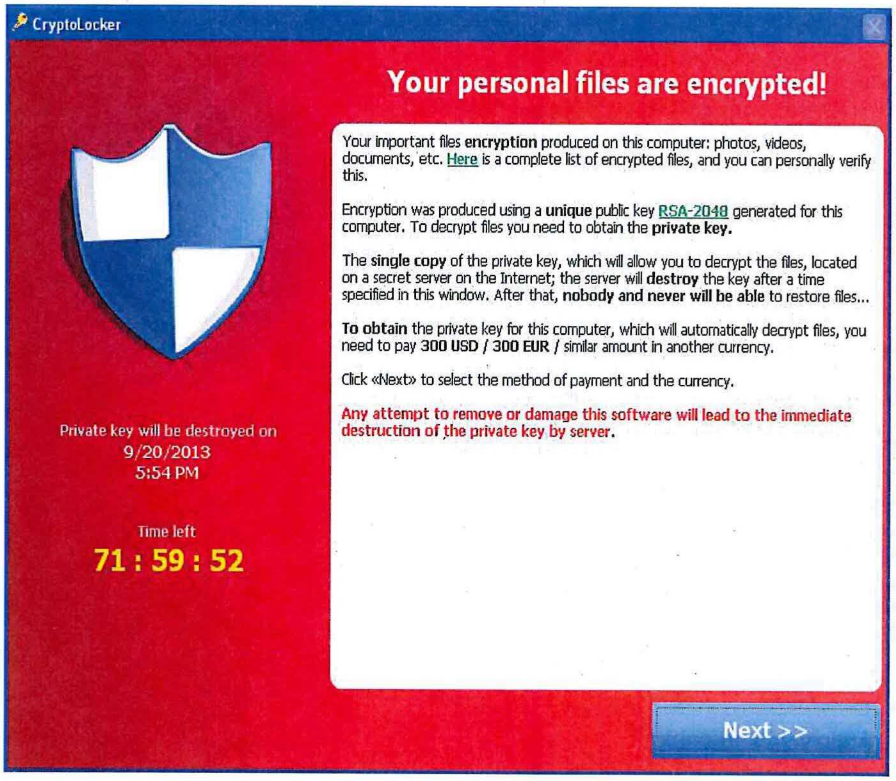
15. Accepting a job as a money mule typically has devastating consequences for the money mule. Not only is the money mule subject to potential criminal liability for money laundering, but mules are frequently held responsible for repaying all of the stolen money that has transited their accounts. Additionally, many banks will apply significant scrutiny to any further banking activity by the mule.

C. Cryptolocker

16. In the course of my GOZ investigation, I have become knowledgeable about the malware program known as Cryptolocker. Cryptolocker is a malicious program designed to extract ransom payments from victims. After infecting a computer, Cryptolocker contacts a server managed by the defendants and then encrypts files on the infected computer's hard drive. Once the victim's files have been encrypted, Cryptolocker displays a splash screen on the

[1] It is difficult to tie recruitment emails to specific botnets, and this email represents a general mule-recruitment solicitation.

victim's computer that demands payment of a ransom in exchange for the private key that can decrypt the victim's files. An image of the ransom notice splash screen displayed to victims appears below:



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
9/20/2013
5:54 PM

Time left
71 : 59 : 52

17. The Cryptolocker ransom, which varies in amount, but can reach up to $750 or more, must be paid via anonymous pre-paid cash vouchers like MoneyPak or via the virtual currency Bitcoin. Victims who refuse to pay the ransom face significant data loss, since the encryption algorithm used by the defendants is effectively unbreakable. Victims who agree to pay the ransom typically receive the private key to unlock their files, although there are other forms of ransomware for which victims paying the defendants and never receiving the private key.

18. Cryptolocker first emerged in mid-to-late 2013 and has infected more than 230,000 computers in the ensuing months, including more than 120,000 victims in the United States. Although the number of infected victims who have paid the Cryptolocker ransom is unknown, a reporter who studied the Bitcoin addresses used by the Cryptolocker operators estimates that $27 million in ransom payments were paid by victims between October 15 and December 18, 2013. *See* Violet Blue, *Cryptolocker's Crimewave: A Trail of Millions in Laundered Bitcoin*, ZDNet, Zero Day, http://www.zdnet.com/cryptolockers-crimewave-a-trail-of-millions-in-laundered-bitcoin-7000024579/.

19. Security researchers believe that GOZ is one of the primary delivery methods for Cryptolocker. Among the features built into GOZ is a "user_execute" command that permits the defendants to install additional software onto any GOZ-infected machine. The defendants have used this capability to install Cryptolocker onto numerous computers already infected with GOZ, thereby adding another stream of revenue to their credential theft operation.

III. THE DEFENDANTS

20. A multi-year FBI investigation has revealed that a tightly knit group of cybercriminals based primarily in Russia and Ukraine are responsible for GOZ and Cryptolocker. These individuals have deliberately targeted their malicious software at U.S. individuals and companies. Although the full scope of harm caused by the defendants is impossible to calculate, the best evidence available suggests that the defendants' malicious software has resulted in direct losses to U.S. businesses and individuals more than $100 million, and indirect losses many times higher. Notably, while earlier versions of Zeus were sold to any individuals willing to pay the asking price, GOZ is tightly controlled and not distributed outside the tightly knit group.

21. The defendants have gone to great lengths to conceal their identities and hide from law enforcement. FBI investigation, including Confidential Human Source (CHS) reporting, pen registers and trap and trace devices, interviews of victims and industry experts, the establishment of threat specific industry working groups, search warrants, open source research, historical forum review, requests to foreign governments pursuant to Mutual Legal Assistance Treaties, custodial interrogations of foreign subjects, and real time attack monitoring, has revealed that, among other tactics, the defendants use false identities and online monikers, anonymous internet-based payment systems, and an extensive network of money mules to launder the funds stolen during their high tech bank robberies. Despite these tactics, as described below, the FBI has identified an individual at the very top of the criminal gang responsible for GOZ and Cryptolocker. That individual is Evgeniy Mikhailovich Bogachev of Anapa, Russia.

22. Bogachev was indicted in the Western District of Pennsylvania on May 19, 2014 for violations of 18 U.S.C. §§ 371 (Conspiracy), 1030(a)(2) (Unauthorized access to a protected computer), 1343 (Wire Fraud), 1344 (Bank Fraud); 1956 (Money Laundering) and 1957 (Engaging in monetary transactions in property derived from specified unlawful activity) arising from his leadership role in the GOZ conspiracy. Bogachev is scheduled to be added to the FBI's list of most wanted cyber criminals and a reward will be offered for information leading to his arrest. FBI investigation has determined that Bogachev's postal address is Lermontova Str. 120-101, Anapa, Russian Federation, and that he uses the e-mail address bollinger.evgeniy@yandex.ru.

23. In addition to Bogachev, the FBI has identified a number of other individuals who are part of the criminal enterprise responsible for GOZ and Cryptolocker. These individuals are

known by the online monikers "Temp Special", "Ded", "Chingiz 911" and "mr. kykypyky", and have also been named as defendants in this action. Based on data obtained by the FBI from an underground hacking forum, the FBI has determined that "Chingiz 911" uses the email address charajiang16@gmail.com.

A. Evgeniy Bogachev

24. In the course of its GOZ investigation, the FBI obtained via a Mutual Legal Assistance Treaty request a copy of a server in the United Kingdom that was believed to serve as a communications hub for the operators of GOZ. Subsequent FBI analysis of the UK server revealed that the server played a much larger role than initially believed.

i. Visitcoastweekend.com Website

25. Among other content, the UK server hosted a website called *visitcoastweekend.com,* which was accessible only to authorized users and required the use of a username and password to login. The Frequently Asked Questions page for that website, translated from the original Russian below, detailed the website's function:

> Starting on September 19, 2011, we are beginning to work through the panel where you now find yourselves. [Fraudulent] Money transfers and drop [money mule] managers are synchronizing their work through our panel, which enables a much greater optimization of the work process and increase in the productivity of our work. Starting from this moment, all drop [money mule] managers with whom we are working and all [fraudulent] money transferors who work with us are working through this panel. We wish you all successful and productive work.[2]

[2] The terms in brackets are not the actual words used on the webpage; however, the actual word used was slang and the implied meaning of the term is what the translator has provided in brackets.

26. Among other content, the *visitcoastweekend.com* website hosted a detailed ledger of hundreds of financial transactions that include dates, company names, amounts, responsible criminal party, and an indicator whether the transaction was an ACH payment or a wire transfer.

27. One of the company names in the *visitcoastweekend.com* ledger is of a composite materials company in the Western District of Pennsylvania (Victim Company #1). The ledger lists a wire transfer of $198,234.93, the date October 21, 2011, and an account number at SunTrust Bank.

28. Interviews with senior representatives of Victim Company #1, as well as the review of relevant transactional logs, confirmed that Victim Company #1 was the target of a bank account intrusion that caused $198,234.93 to be wired from its bank account to an account at another U.S. bank on October 20, 2011. The unauthorized wire transfer was initiated using the credentials of two employees at Victim Company #1, both of whom denied any knowledge of the transfer. Subsequent FBI analysis confirmed that the employee credentials used in the theft were stolen from a computer at Victim Company #1 that was infected with GOZ.

29. The FBI has interviewed representatives a number of companies listed in the ledger hosted on the *visitcoastweekend.com* website, and studied fraud reports submitted by banks that match the transactions in this ledger. For all listed companies with respect to which the FBI manually reviewed information in the ledger and compared it to information from either field interviews or bank fraud reporting, the information was an exact match. That analysis led the FBI to conclude that the entries in the ledger are victims of GOZ, and that the ledger was used by the GOZ operators to track their fraudulent bank transfers.

ii. Businessclub Website

30. In addition to the *visitcoastweekend.com* website, the UK server also contained data related to the website *work.businessclub.so* (the "Businessclub website"). FBI analysis of the Businessclub website revealed a robust ticket system relating to the daily technical operation of the bot system. A ticket system is a method of tracking various information technology projects from a central vantage point. One common example is the process by which a computer "help desk" might track a problem as it is reported by a user, assigned to a technician, and resolved.

31. Users and administrators used the ticket system in the Businessclub website to identify deficiencies in the GOZ botnet or to request improvements. These "tickets" would then be assigned to personnel in a support role, such as Chingiz 911 and Ded, who would fix the problem and update the ticket when it was resolved. The website also tracked the status of assigned projects.

iii. Bogachev's ties to the UK Server, visitcoastweekend.com and the BusinessClub website

32. A CHS advised the FBI that a GOZ administrator was using an email address hosted by a Russian provider. To pursue this lead, a search warrant was served on a U.S. provider of online services (hereinafter, "Service Provider") for records related to that email address. The records produced in response to the search warrant revealed an account in the name of Evgeniy Bogachev and a comprehensive log of IP addresses that were used to access Bogachev's account from 2010 through October 2013.

33. The FBI compared the IP addresses from Bogachev's Service Provider account with a series of server logs obtained from the UK GOZ server. Specifically, the FBI compared

the Service Provider IP data with three other sources: the logs from the Administrative Panel for the UK server, the logs for *visitcoastweekend.com*, and the logs for the Businessclub website. This analysis revealed thousands of instances in which the same IP address tied to Bogachev's Service Provider account appeared in server activity logs for the Administrative Panel for the UK Server, *visitcoastweekend.com*, and the Businessclub website, during distinct time periods.

34. Further analysis of the UK server logs linked the Bogachev-connected IP addresses used to access the Administrative Panel of the UK Server and the Businessclub website to the same computer. The FBI made this connection by studying a digital footprint known as a "user agent string." When connecting to a website, a user's web browser transmits a user agent string – information about the computer on which the browser is running. This information typically includes the computer's operating system and version, as well as information about the browser itself, including the version number. Based upon my training and experience, user agent strings can be useful, particularly in combination with other information like IP addresses, for tracking individuals through log files. The FBI compared the user agent string information for numerous logins to the Administrative Panel of the UK Server and the Businessclub website from IP addresses previously tied to Bogachev. This analysis confirms that the same user agent string appears again and again connected to these logins.

35. Based on this consistent pattern of overlapping IP addresses and user agent strings, the FBI assesses that that Bogachev was the individual utilizing and managing the GOZ infrastructure. Moreover, based on the fact that Bogachev had elevated Administrative access to the critical UK GOZ server, the FBI assesses that he is a leader of the GOZ conspiracy. Notably, GOZ is a very closely held criminal operation. While the prevalent model for computer malware

is for owners to sell outright the malware product and to receive additional payment for troubleshooting and product updates, examination of the database files upon which *businessclub.so* and *visitcoastweekend.com* are built indicates that a disproportionate amount of power over GOZ is wielded by a small number of administrative users. In this context, Bogachev's Administrative access further indicates that he is one of the principal leaders of the GOZ conspiracy.

iv. Bogachev's Use of the "Pollingsoon" Moniker

36. A historical copy of an underground hacking online forum known as CardingWorld was obtained by the FBI pursuant to an MLAT request. The FBI analyzed user activity for the forum user "Pollingsoon," who the FBI determined has participated for years in the forum. On many dates beginning in 2010, Pollingsoon interacted on Cardingwold from the same IP address that appears in the transactional logs on those dates for Bogachev's Service Provider account. This correlation strongly indicates that the same individual was accessing Bogachev's Service Provider account and interacting on CardingWorld as Pollingsoon, and by extension, that Bogachev was interacting as Pollingsoon.

37. The FBI's review of the CardingWorld forum information revealed that, on multiple occasions, Pollingsoon has claimed to be the author of the Zeus malware in private messages sent to other members of the forum. That review further revealed that in other private messages, Pollingsoon has stated that he is "Slavik" and provided ICQ numbers[3] that, according to an open search of the ICQ website, are registered with the first name of "Slavik."

[3] ICQ is an instant messaging platform that allows participant to communicate with each other in near real time. Each ICQ subscriber has a unique ICQ number, which is the rough equivalent of a telephone number. A user seeking to communicate with another ICQ subscriber must know the ICQ number of that subscriber in order to

38. Slavik's central role in the development and sale of the original Zeus malware led the Microsoft Corporation to name Slavik as a defendant in its March 2012 civil suit brought against numerous online monikers that Microsoft alleged to be the perpetrators of Zeus. *See Microsoft Corp. v. John Does 1-39*, Civil Case No. 12-01335 (E.D.N.Y. 2013). That suit concluded on November 29, 2012, when Judge Sterling Johnson of the Eastern District of New York entered a permanent injunction against Slavik and other aliases ordering them to, *inter alia*, stop infecting Microsoft Windows customers with malicious software and to stop enlisting Microsoft Windows customers into botnets.

39. Investigation by other law enforcement agencies as well as analysis of diction patterns indicates that the Slavik moniker and ICQ addresses may have been shared among two or more individuals and it is possible that others had substantial roles in developing and marketing earlier versions of Zeus as well as GOZ. Based upon the complexity and technical sophistication of Zeus, and of the GOZ variant in particular, it is likely that Bogachev had substantial assistance in the development and marketing of the malware products. Based upon my training and experience, I know that the operation of most botnets requires teams of people. Botnets such as GOZ can directly employ upwards of 50 people. Based on the foregoing—particularly the strong IP address and user agent string correlation—the FBI believes that Bogachev is a leader of the GOZ botnet and remains a senior member of the criminal enterprise that developed and deployed the earlier versions of Zeus and GOZ.

communicate with that user.

v. Relationship of Bogachev to Cryptolocker

40. In November 2013, the FBI located a server in the United States that was hosting the Cryptolocker malware and acting as a command and control server in the Cryptolocker infrastructure. On November 13, 2013, a court-approved pen register/trap and trace device was installed on the command and control server. The results of the monitoring showed that the server was initiating connections to a second level command and control server in the United Kingdom (UK). Law enforcement authorities in the UK initiated monitoring on the UK-based second level Cryptolocker command and control server. Their monitoring revealed that the majority of the data from the UK command and control server was directed to and from a server located in Luxembourg with the IP address 146.185.239.64.

41. In cooperation with Luxembourg law enforcement agencies, pursuant to an MLAT request, the FBI analyzed the contents of this server, discovering HTTP access logs that showed which users were accessing this server. The access logs contained entries for an administrative account utilizing the Switzerland-based IP address 46.28.204.78. This IP address appeared multiple times throughout the logs, including during May 2013. The IP address appears in Bogachev's Service Provider account, referenced above, during the same time period. For example, on May 29, 2013, the same IP address accessed the Luxembourg Cryptolocker server and Bogachev's account with the Service Provider within a window of less than three hours. Because the Cryptolocker server administrative account in Luxembourg was accessed on multiple occasions from the same computer or device that accessed Bogachev's service provider account, and that computer or device accessed both the Cryptolocker server and Bogachev's

Service Provider account within the same time period, the FBI assesses that Bogachev was the individual accessing the Cryptolocker server at an administrative level.

B. The Nickname Defendants

42. The FBI's review of the data associated with the Businessclub website revealed a list of registered users with the authority to access the site, as well as their assigned roles. The user list does not include real names, but rather lists online monikers. Based on this information, the FBI has concluded that four individuals are likely to have sufficient control over the GOZ botnet to enable them to comply with a TRO from this Court ordering them to halt the scheme. These individuals use the monikers "Temp Special," "Ded," "Chingiz 911," and "mr. kykypyky." The login name for the user "Chingiz 911" on the work.businessclub.so server is "Chingiz."

C. Need for *Ex Parte* Relief

43. Based on my training and experience, including both my investigation of GOZ and other cyber criminal entities and my knowledge of how GOZ is operated, if the defendants were to be notified in advance of the planned disruption, they could and would take simple, rapid steps to blunt or defeat the Government's planned disruption. Such steps would likely include relocating their servers and command and control infrastructure and/or making significant changes to the intermediary communication protocols, which would not take extensive time or effort.

a. GOZ and Cryptolocker are rapidly evolving malware sets, and the defendants are able to easily change the malware. Nearly the entire GOZ botnet can be updated within 24 hours. The GOZ botnet has been updated in this manner many times in response to the activities of industry researchers such as sinkholing or the publication of research papers detailing GOZ vulnerabilities.

[** REDACTED **]

D. Need to Redact Operational Information

44. The sources and methods used to conduct the technical disruption operation described will remain highly sensitive, even after the operation ends and the indictment and other court papers are unsealed. Exposing those sources and methods would jeopardize future efforts to disrupt similar criminal activity.

45. Specifically, the descriptions of specific vulnerabilities of the defendants' malware and the technical means by which the Government intends to exploit those vulnerabilities will remain highly sensitive. Making public the vulnerabilities that the Government has identified and the means by which the operation will exploit those vulnerabilities would provide the defendants, and other malware designers, information they would use to craft malware that is even more resistant to disruption than the malware at issue in this case.

IV. GOZ AND CRYPTOLOCKER HAVE HARMED VICTIMS IN THIS DISTRICT AND THROUGHOUT THE UNITED STATES

46. GOZ and Cryptolocker have caused enormous injury in this District and throughout the United States. Although it is impossible to fully quantify the losses these two malicious programs have caused, the paragraphs below provide the court with an overview of the scope of injury at issue.

A. GOZ

47. Based on its investigation to date, the FBI estimates that GOZ has caused more than $100 million in direct loss since GOZ was first detected in September 2011. The FBI further assesses that, because victims are rarely able (without the technical assistance of the FBI) to directly connect their losses to the theft of their banking credentials by GOZ, these estimates understate the actual losses that GOZ has caused.

48. As noted above, GOZ is programmed to defeat the added safeguards that banks place on corporate bank accounts, including one-time authorization codes. Accordingly, the defendants often use GOZ to target lucrative corporate bank accounts, especially those belonging to small and mid-sized businesses. The impact of these attacks on these organizations is often devastating, as illustrated by the cross-section of GOZ victims discussed below:

a. In October 2011, a composite materials company in the Western District of Pennsylvania had more than $198,000 wired from its bank account. Although the bank's records show that the wire was authorized by two company employees, the employees denied initiating or approving the wire transfer. Subsequent FBI investigation revealed that an employee at the materials company had unknowingly infected a company computer with GOZ by clicking on a link in an email. GOZ was then used to steal the credentials of two company employees authorized to approve wire transfers. Those credentials were then used to initiate the fraudulent wire transfer.

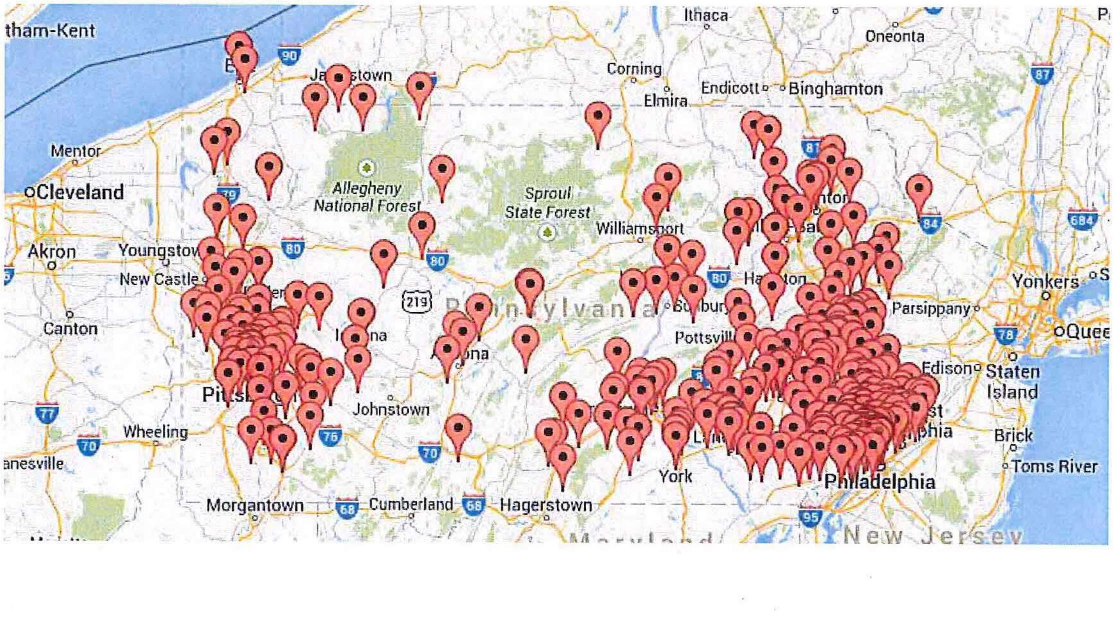
b. In February and March 2012, an Indian tribe in Washington State had more than $277,000 wired from its bank account to overseas accounts. Subsequent FBI investigation revealed that a computer at the tribe's accounting firm was infected with GOZ, and that the fraudulent wire transfers were initiated using credentials stolen from the accounting firm.

c. In April 2012, the Director of Finance for three assisted living facilities in eastern Pennsylvania unknowingly infected his computer with GOZ via a malicious email. Shortly thereafter, a total of $190,800 in fraudulent ACH transfers was initiated from the facilities' corporate bank account.

d. In November 2012 a regional bank in northern Florida had nearly seven million dollars fraudulently wired out of one of its accounts. The bank maintained an account at a larger correspondent bank – a bank that provides services to other banks rather than to businesses or individuals. On November 6, 2012, a fraudulent wire in the amount of $6,984,672 was initiated from the correspondent bank account to an account in Switzerland. Although the correspondent bank's records show that the wire was initiated by an employee of the Florida bank, that employee denied initiating or authorizing the wire transfer. Subsequent FBI investigation confirmed that a computer at the Florida bank was infected with GOZ, and that the infected computer was used to steal the credentials that were used to initiate the fraudulent transfer.

49. Additional insight about the impact of GOZ on this District, and the Commonwealth of Pennsylvania as a whole, can be gained by studying GOZ infection data. The infection map below was created by a private security researcher who has extensively studied the GOZ botnet and was able to plot the IP addresses of GOZ infected computers on a single day in May 2013.

50. The map shows a large number of GOZ infections in this District, and in Pennsylvania as a whole.



B. Cryptolocker

51. By monitoring connection attempts to domain names used by Cryptolocker, security researchers are able to estimate the total number of Cryptolocker infections. This data shows that as of April 2014, Cryptolocker has infected more than 234,000 computers, and that more than half of those infections – nearly 120,000 – occurred in the United States.

52. It is estimated that tens of millions of dollars in ransom payments have been paid by Cryptolocker victims. Although this figure is substantial, it is a small fraction of the actual losses caused by Cryptolocker. FBI interviews with numerous Cryptolocker victims demonstrate that many victims are either unable or unwilling to pay the ransom demanded by the defendants. As a result, these victims often end up losing their data. While it is difficult to assign a dollar value to these losses, the victim narratives below help illustrate the magnitude of the loss:

a. In November 2013, an employee at an insurance company in Pittsburgh, Pennsylvania opened an attachment to an email that purported to originate from a major U.S. bank. The attachment infected the employee's work computer with Cryptolocker. Cryptolocker encrypted the files on the employee's computer and displayed a splash screen demanding that a ransom be paid in order to return the encrypted files to a readable state. The employee subsequently learned that because his computer was connected to the company's network at the time of infection, Cryptolocker was able to access the company's network and encrypt critical business files. The company was able to repair the damage by using backup files, but was forced to send employees home while the repair work was completed. The company estimates its total loss at $70,000.

b. In October 2013, an employee of a restaurant operator in Florida opened an attachment to an email that appeared to originate from inside the company. The attachment infected the employee's work computer with Cryptolocker, which encrypted the files on her computer as well as a shared network drive. More than ten thousand files were encrypted, including the contents of the company's team training, franchise, and recipe folders. The company's head of Information Technology estimates that remediating the Cryptolocker infection has cost the company $30,000.

c. In November 2013, a computer at the Swansea Police Department in Massachusetts ("SPD") was infected with Cryptolocker. Because the infected computer was connected to the SPD's network, Cryptolocker was able to access and encrypt the SPD's main file server. Files encrypted on this server included administrative documents, investigative materials, and seven years' worth of digital photo mug shots. To recover these critical files, the SPD was forced to pay the $750 ransom demanded by Cryptolocker.

d. On April 4, 2014, an employee at a pest control company in North Carolina unwittingly infected the company's computers with Cryptolocker after opening an email attachment. Cryptolocker promptly traversed the company's network and encrypted the company's most critical files, including its customer database and schedule of appointments. Cryptolocker also encrypted the company's backup server. The company hired a computer forensics firm to recover the encrypted data, but no data could be saved. The owner of the company estimates that the Cryptolocker infection has cost his company approximately $80,000 to date and is contemplating whether the losses incurred will force him to lay off employees.

V. THE UNITED STATES IS PREPARED TO DISRUPT THE GOZ BOTNET AND CRYPTOLOCKER

53. The FBI has developed a comprehensive technical plan to disrupt both the GOZ botnet and Cryptolocker. A detailed review of the technical disruption effort and subsequent remediation campaign is provided below.

A. GOZ

54. The GOZ botnet is widely believed to be the most advanced in existence and one of the most difficult to remediate. This is primarily due to the botnet's decentralized command and control infrastructure, which makes the GOZ botnet impervious to traditional disruption techniques such as seizing key command and control servers or domain names.

55. To successfully disrupt the GOZ botnet requires a comprehensive technical approach that severs the three separate communications channels used by the defendants to control the infected computers within the botnet. The technical operations planned against each

of these three communications channels – the Peer Layer, the Proxy Layer, and the Domain Generation Algorithm – are discussed below.

[** REDACTED **]

iii. DGA Domains

56. The final step to liberating infected computers from the GOZ botnet is to control the Internet domains generated by GOZ's Domain Generation Algorithm ("DGA"). The DGA is yet another failsafe built into the GOZ code that is designed to harden the GOZ network against communications failures and disruption efforts. The DGA generates a list of 1,000 domain names, which consist of lengthy combinations of letters – acawktkhtdfqfumnttoaydwckn, for example – combined with one of six top level domains ("TLDs"): .com, .net, .org, .biz, and .info, which are controlled by Registries in the United States and .ru, which is TLD for the Russian Federation.

57. At least once every week,[4] the GOZ code picks a random starting point on the list of 1,000 domain names generated by the DGA and attempts to connect to that domain. If no response is received, the GOZ code will move to the next domain, and proceed sequentially through the list until a successful connection attempt is made. If attempts to reach all 1,000 of the domains fail, the GOZ code will try again the next week using a fresh list of 1,000 domains generated by the DGA. After connecting to a DGA domain, GOZ requests a Peer List – a list of other infected bots in the GOZ network. Once the Peer List is received, GOZ appends a select number of the new Peers to the existing list of Peers maintained on each infected computer.

[4] In addition to the weekly check-in, a Peer will seek a Peer List from the DGA domains whenever there are fewer than 25 peers on its Peer List or the Peer fails to learn of any new Peers during Peer verification.

58. In order to prevent the defendants from using the DGA to recapture Peers at the substitute server, it is essential that the domains generated by the DGA be kept out of the defendants' hands.[5] The TRO sought as part of this action denies the defendants these domains through two provisions: 1) an order to the Domain Registries responsible for the U.S.-based TLDs requiring them to redirect connection attempts to DGA-generated domains to the substitute server; and 2) an order directing the largest domestic ISPs to block connection requests to the malicious .ru domains generated by the DGA.

B. Cryptolocker

59. The technical operation against Cryptolocker bears much in common with the operation against GOZ, but is far less complex. There are three essential elements.

60. The first step will be to seize key servers in the Cryptolocker infrastructure, which are located in Canada, Ukraine, and Kazakhstan. On or about May 30, 2014, the FBI's foreign law enforcement partners will seize these servers in coordination with the FBI's operation.

61. The second and third steps in the operation target the DGA used by Cryptolocker. Like GOZ, Cryptolocker uses a DGA, although in a slightly different fashion. The Cryptolocker DGA generates 1,000 domain names per day across seven TLDs. Immediately upon infecting a computer, Cryptolocker attempts to connect to domains that are hardcoded (written directly) into the malware. If that connection attempt fails, Cryptolocker runs the DGA and attempts to connect to the domains generated by the DGA. Testing of Cryptolocker has shown that Cryptolocker must connect to one of these command and control domains before it will encrypt

[5] The DGA has been reverse engineered by security researchers and as a result, the FBI is able to accurately predict which domains will be generated for each week.

files on the infected computer. If these domains are blocked, Cryptolocker should not be able to initiate its encryption function.

62. To add to the disruption caused by the infrastructure disruptions, this action seeks a TRO that prevents the defendants from registering and using the hardcoded domains and the Cryptolocker DGA domains. To keep these domains out of the defendants' hands, the requested TRO contains two provisions: 1) an order to the Domain Registrars responsible for the U.S.-based TLDs used by Cryptolocker that prohibits the Registrars from allowing these domains to be registered; and 2) an order directing the largest domestic ISPs to block connection requests to the .ru domains generated by the Cryptolocker DGA.[6]

I declare under penalty of perjury under the law of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed this 27th day of May, 2014, in Pittsburgh, Pennsylvania.

/s/ Elliott Peterson
Elliott Peterson
Special Agent
Federal Bureau of Investigation

[6] There is one downside to disrupting the Cryptolocker infrastructure and blocking the Cryptolocker DGA domains: once the operation commences, computers that have already been infected and encrypted by Cryptolocker will be cut off from the network. As a result, it will be impossible for these users to pay the Cryptolocker ransom and obtain the private key to decrypt their computers.

Although it is difficult to estimate the number of users that will be negatively impacted by the Cryptolocker disruption, the Government believes the number will be small. After encrypting victim computers, Cryptolocker informs its victims that the ransom must be paid within 72 hours. To highlight the urgency, Cryptolocker displays a countdown clock on victims' screens warning of the deadline. It is reasonable to assume that the overwhelming majority of victims take this warning at face value and decide whether or not to pay the Cryptolocker ransom within the 72 hour period. Accordingly, the pool of victims that wish to pay the Cryptolocker ransom but will be blocked from doing so because of the technical operation will be limited to those who have been infected within 72 hours of the operation. Some of the victims within this pool will have already paid the ransom, which will further reduce the number of impacted victims.